630

Congress of the United States
Washington, DC 20510

PSHSB
Public Safety
Preparedness

June 17, 2015

The Honorable Thomas Wheeler
Chairman
Federal Communications Commission
445 12th Street SW,
Washington, DC 20554

Dear Mr. Chairman:

As you are aware, our Nation faces a considerable cyber threat. That threat continues to grow in terms of both sophistication and frequency, from foreign state actors, criminals, hacktivists, and terrorists who will not hesitate to steal, destroy, or vandalize our cyber assets.

Cyber criminals can utilize a variety of techniques to gain access to our computer networks but wireless networks are particularly vulnerable to attack. Because wireless networks are ubiquitous—present in homes, businesses of all sizes, restaurants, hotels, and airports—and do not require physical access for a connection, securing them is a unique challenge. For example, wireless networks are especially vulnerable to man-in-the-middle attacks, denial of service attacks, and eavesdropping.[1]

No one is immune from cyber incidents, as evidenced by recent intrusions at JP Morgan Chase, Anthem, Home Depot, Target, the White House and, most recently, the Office of Personnel Management. To protect our Nation and its citizens, the Federal Government must be a leader in best practices on cybersecurity and ensure the legal and regulatory environments our businesses operate in provide them the flexibility they need to secure their networks against attack. In discharging that leadership role it is imperative that government agencies give consistent guidance and support to businesses in meeting and defeating cybersecurity threats.

Unfortunately, we are concerned this goal is not being met due to conflicting information from the Department of Homeland Security (DHS) and the Federal Communications Commission (FCC) regarding the use of Wireless Intrusion Detection Systems and Wireless Intrusion Prevention Systems (WIDS/WIPS) to protect wireless networks and users from cyber-attacks.

---

[1] *See, e.g.*, MURUGIAH SOUPPAYA & KAREN SCARFONE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-153, GUIDELINES FOR SECURING WIRELESS LOCAL AREA NETWORKS (WLANS) (DRAFT) 8–9 (2011).

In September 2011, DHS's National Cyber Security Division issued the *Wireless Local Area Network (WLAN) Reference Architecture* in which it discussed the importance of WIDS/WIPS.[2] Because WIDS/WIPS can "detect" and "take countermeasures against the WLAN [wireless local area network] threats," the reference architecture concluded that "WIDS/WIPS deployment is critical to the WLAN security and operation, and therefore is required by the WLAN Reference Architecture."[3]

However, on January 27, 2015, the FCC's Enforcement Bureau issued an Enforcement Advisory which suggests that a WLAN operator violates federal law when using WIDS/WIPS to "block" a wireless network access point that is being used to launch a cybersecurity attack against the operator's network or its customers.[4] The agency also intimated that equipment with WIDS/WIPS functionality is the equivalent of a "jammer," the operation of which is unlawful.[5]

To better understand the coordination between the FCC and DHS and other agencies on this matter, and your position on use of WIDS/WIPS to protect networks against cyber-attack, we request you provide answers to the following questions:

Interagency Coordination

(1) With what other agencies, including DHS and the National Institute of Standards and Technology (NIST), did the FCC coordinate in developing the Enforcement Advisories referenced above and how did it coordinate with those agencies?

Consistency with Existing Federal Cybersecurity Initiatives

(2) The *WLAN Reference Architecture* "offers best practices" for WLAN security. Is there any policy reason the private sector should not be encouraged to follow DHS's guidance in protecting their networks?

(3) What recommendations would you offer to a WLAN operator in the private sector about the use of WIDS/WIPS in protecting its network from cybersecurity threats, given the apparent conflict between DHS's *WLAN Reference Architecture* and the FCC Enforcement Advisories referenced above?

---

[2] DEP'T OF HOMELAND SEC., NAT'L CYBER SEC. DIV., WIRELESS LOCAL AREA NETWORK (WLAN) REFERENCE ARCHITECTURE § 4.4 (2011).

[3] *Id.*

[4] Fed. Commc'n Comm'n, DA 15-113, Enforcement Advisory: WARNING: Wi-Fi Blocking is Prohibited (Jan. 27, 2015).

[5] *See* Fed. Commc'n Comm'n, DA 12-347, Enforcement Advisory: Cell Jammers, GPS Jammers, and Other Jamming Devices (Mar. 6, 2012).

(4) Would the use of WIDS/WIPS to detect and stop a cybersecurity threat be consistent with the use of mitigation efforts "to prevent expansion of an event, mitigate its effects, and eradicate the incident," as recommended in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*?[6]

(5) Would the use of WIDS/WIPS to detect and stop a cybersecurity threat be consistent with the use of "Intrusion Detection-Protection" to prevent, mitigate, respond, and recover from "cyber-attack incidents," as recommended in the Communications Security, Reliability, and Interoperability Council's *Cybersecurity Risk Management and Best Practices* report?[7]

Permitted and Non-Permitted Uses of WIDS/WIPS

(6) Under what circumstances is the use of WIDS/WIPS permitted and under what circumstances is it prohibited?

(7) If a malicious actor sets up a wireless network access point designed to spoof another, legitimate access point in order to steal personal information from users of the legitimate access point,[8] is the operator of the legitimate access point permitted to use WIDS/WIPS to block that access point and thereby protect unsuspecting users from associating to it?

(8) If a malicious actor sets up a wireless access point that is being used to launch attacks against another wireless network, is the operator of the wireless network being attacked permitted to use WIDS/WIPS to block that access point in order to protect its network?

(9) Are Federal agencies operating WLANs required or advised to utilize WIDS/WIPS to protect their networks from cybersecurity incidents? If so, why should the private sector be prohibited from using the same technology to protect their networks from cybersecurity incidents?

We request your responses to these questions as soon as possible, but no later than 5:00 p.m. on July 2, 2015.

---

[6] NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 34 (2014) [hereinafter NIST CYBERSECURITY FRAMEWORK] (Mitigation RS.MI).

[7] COMMC'N SEC., RELIABILITY AND INTEROPERABILITY COUNCIL, WORKING GROUP 4, CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES: FINAL REPORT 296–301, 308 (2015) [hereinafter CSRIC BEST PRACTICES].

[8] For example, a malicious actor might setup a wireless access point in a hotel with the name of the hotel as part of the access point name (SSID) or use a spoofed MAC address of a valid station or access point in the hotel's network, to deceive users into thinking the hotel is operating the access point and connecting to it.

If you have any questions about this request, please contact William McKenna of Chairman Johnson's staff at (202) 224-3288 or William_McKenna@hsgac.senate.gov and Brett DeWitt of Chairman McCaul's staff at (202) 226-8417 or Brett.DeWitt@mail.house.gov. Thank you again for your assistance in this matter.

Sincerely,

RON JOHNSON
Chairman
Senate Committee on Homeland
Security & Governmental Affairs

MICHAEL T. MCCAUL
Chairman
House Committee on
Homeland Security

Cc: The Honorable Jeh Johnson, Secretary, Department of Homeland Security
The Honorable Thomas R. Carper, Ranking Minority Member, Senate Committee on Homeland Security & Governmental Affairs
The Honorable Bennie G. Thompson, Ranking Minority Member, House Committee on Homeland Security
The Honorable Mignon Clyburn, Commissioner, Federal Communications Commission
The Honorable Jessica Rosenworcel, Commissioner, Federal Communications Commission
The Honorable Ajit Pai, Commissioner, Federal Communications Commission
The Honorable Michael O'Rielly, Commissioner, Federal Communications Commission

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

June 29, 2015

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Johnson:

Thank you for your letter concerning the Federal Communications Commission's position on the use of Wireless Intrusion Detection Systems and Wireless Intrusion Prevention Systems (WIDS/WIPS) to protect wireless networks and users from cyberattacks. Your letter raises important legal and policy questions that underscore the need to balance the practical needs of network operators to protect their systems with consumers' expectation of easy utilization of Wi-Fi access points. The FCC is committed to striking the right balance between ready access to unlicensed spectrum and effective cyber defense. Accordingly, our enforcement activity in this arena has focused on circumstances where companies are not "defending" their networks, but instead are using these capabilities to knowingly deny legitimate users access to shared unlicensed spectrum.

Your letter expresses concern regarding a perceived tension between the FCC Enforcement Bureau's January 27, 2015 Enforcement Advisory on Wi-Fi blocking,[1] and the Department of Homeland Security's *Wireless Local Area Network (WLAN) Reference Architecture* publication regarding the use of WIDS/WIPS by Federal agencies.[2] Although the Commission's jurisdiction is limited to non-federal uses of the radiofrequency spectrum, we understand the two documents to be consistent in their positions that network operators should not use "blocking" to interfere with the operation of independent wireless networks.

As a general matter, Enforcement Advisories serve to educate businesses and consumers about what the Communications Act of 1934, as amended, and the FCC's rules require, the purpose and importance of those laws and rules, and the consequences of failure to comply. Enforcement Advisories thus simply illuminate issues for the benefit of the public and entities that may be subject to the Commission's jurisdiction.

---

[1] *See* https://apps.fcc.gov/edocs_public/attachmatch/DA-15-113A1.pdf ("FCC ENFORCMENT ADVISORY—WARNING: Wi-Fi Blocking is Prohibited"). Your letter also references an Enforcement Advisory issued on March 6, 2012. *See* https://apps.fcc.gov/edocs_public/attachmatch/DA-12-347A1.pdf ("FCC CONSUMER ALERT: Using or Importing Jammers is Illegal").

[2] Dep't of Homeland Sec., Nat'l Cyber Sec. Div., Wireless Local Area Network (WLAN) Reference Architecture sect. 4.4 (2011) (DHS Reference Architecture).

The Enforcement Advisory referenced in your letter provided narrowly tailored guidance regarding behavior that is prohibited by Section 333 of the Communications Act, which states that "[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this Act or operated by the United States Government." The Enforcement Advisory did not change policy regarding the legitimate use of WIDS/WIPS by non-federal users and does not address any practices of federal government network operators, over which the FCC has no statutory jurisdiction.

The Enforcement Advisory states that no hotel, convention center, or other commercial establishment or the network operator providing services at such establishments, may intentionally block or disrupt personal Wi-Fi hot spots on such premises, including as part of an effort to force consumers to purchase access to the property owner's Wi-Fi network. The Enforcement Bureau issued this advisory following its 2014 Consent Decree with Marriott International, Inc., in which the company deployed a Wi-Fi deauthentication protocol to deliberately and indiscriminately block consumers who sought to connect to the Internet using their own personal Wi-Fi hot spots. In that case, Marriott admitted that the customers it blocked did not pose a security threat to the Marriott network and agreed to settle the investigation. Because the FCC had received several complaints that other commercial Wi-Fi network operators might be disrupting the legitimate operation of personal Wi-Fi hot spots, the Enforcement Bureau issued the advisory to provide more information to businesses and consumers.

The Enforcement Advisory is consistent with the DHS document. For example, the DHS document states that a federal agency should recognize that there may be independent Wi-Fi networks in the vicinity of the agency's operations and the agency should not configure its WIDS/WIPS to automatically block them. Indeed, the DHS document calls for federal agencies to address and plan for legitimate external Wi-Fi use, and notes that WIDS/WIPS have features that enable a security specialist to monitor legitimate threats while identifying non-threats caused by these cases of overlapping local area networks.

The FCC recognizes and values the significant experience that DHS and other federal partners bring to this crucial cybersecurity discussion, and the FCC and DHS regularly share expertise in support of our independent yet complementary missions. The FCC enjoys a longstanding and mutually-beneficial working relationship with DHS and other interagency partners.

Thank you for your interest in this matter. The security of our nation's communications network is vital to both private and public sectors. We recognize that there is additional work to do to define defensible best practices for shared unlicensed bands, and we look forward to working with our federal partners to develop these best practices.

Sincerely,

Tom Wheeler

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

June 29, 2015

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, D.C. 20515

Dear Chairman McCaul:

Thank you for your letter concerning the Federal Communications Commission's position on the use of Wireless Intrusion Detection Systems and Wireless Intrusion Prevention Systems (WIDS/WIPS) to protect wireless networks and users from cyberattacks. Your letter raises important legal and policy questions that underscore the need to balance the practical needs of network operators to protect their systems with consumers' expectation of easy utilization of Wi-Fi access points. The FCC is committed to striking the right balance between ready access to unlicensed spectrum and effective cyber defense. Accordingly, our enforcement activity in this arena has focused on circumstances where companies are not "defending" their networks, but instead are using these capabilities to knowingly deny legitimate users access to shared unlicensed spectrum.

Your letter expresses concern regarding a perceived tension between the FCC Enforcement Bureau's January 27, 2015 Enforcement Advisory on Wi-Fi blocking,[1] and the Department of Homeland Security's *Wireless Local Area Network (WLAN) Reference Architecture* publication regarding the use of WIDS/WIPS by Federal agencies.[2] Although the Commission's jurisdiction is limited to non-federal uses of the radiofrequency spectrum, we understand the two documents to be consistent in their positions that network operators should not use "blocking" to interfere with the operation of independent wireless networks.

As a general matter, Enforcement Advisories serve to educate businesses and consumers about what the Communications Act of 1934, as amended, and the FCC's rules require, the purpose and importance of those laws and rules, and the consequences of failure to comply. Enforcement Advisories thus simply illuminate issues for the benefit of the public and entities that may be subject to the Commission's jurisdiction.

---

[1] *See* https://apps.fcc.gov/edocs_public/attachmatch/DA-15-113A1.pdf ("FCC ENFORCMENT ADVISORY—WARNING: Wi-Fi Blocking is Prohibited"). Your letter also references an Enforcement Advisory issued on March 6, 2012. *See* https://apps.fcc.gov/edocs_public/attachmatch/DA-12-347A1.pdf ("FCC CONSUMER ALERT: Using or Importing Jammers is Illegal").

[2] Dep't of Homeland Sec., Nat'l Cyber Sec. Div., Wireless Local Area Network (WLAN) Reference Architecture sect. 4.4 (2011) (DHS Reference Architecture).

The Enforcement Advisory referenced in your letter provided narrowly tailored guidance regarding behavior that is prohibited by Section 333 of the Communications Act, which states that "[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this Act or operated by the United States Government." The Enforcement Advisory did not change policy regarding the legitimate use of WIDS/WIPS by non-federal users and does not address any practices of federal government network operators, over which the FCC has no statutory jurisdiction.

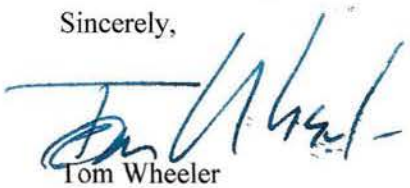
The Enforcement Advisory states that no hotel, convention center, or other commercial establishment or the network operator providing services at such establishments, may intentionally block or disrupt personal Wi-Fi hot spots on such premises, including as part of an effort to force consumers to purchase access to the property owner's Wi-Fi network. The Enforcement Bureau issued this advisory following its 2014 Consent Decree with Marriott International, Inc., in which the company deployed a Wi-Fi deauthentication protocol to deliberately and indiscriminately block consumers who sought to connect to the Internet using their own personal Wi-Fi hot spots. In that case, Marriott admitted that the customers it blocked did not pose a security threat to the Marriott network and agreed to settle the investigation. Because the FCC had received several complaints that other commercial Wi-Fi network operators might be disrupting the legitimate operation of personal Wi-Fi hot spots, the Enforcement Bureau issued the advisory to provide more information to businesses and consumers.

The Enforcement Advisory is consistent with the DHS document. For example, the DHS document states that a federal agency should recognize that there may be independent Wi-Fi networks in the vicinity of the agency's operations and the agency should not configure its WIDS/WIPS to automatically block them. Indeed, the DHS document calls for federal agencies to address and plan for legitimate external Wi-Fi use, and notes that WIDS/WIPS have features that enable a security specialist to monitor legitimate threats while identifying non-threats caused by these cases of overlapping local area networks.

The FCC recognizes and values the significant experience that DHS and other federal partners bring to this crucial cybersecurity discussion, and the FCC and DHS regularly share expertise in support of our independent yet complementary missions. The FCC enjoys a longstanding and mutually-beneficial working relationship with DHS and other interagency partners.

Thank you for your interest in this matter. The security of our nation's communications network is vital to both private and public sectors. We recognize that there is additional work to do to define defensible best practices for shared unlicensed bands, and we look forward to working with our federal partners to develop these best practices.

Sincerely,



Tom Wheeler